UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,983	03/15/2004	G. Glenn Henry	CNTR.2073	1410

23669 7590 04/16/2008
HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
04/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/800,983	HENRY ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *07 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 17-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 17-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/11/2007, 10/19/2007, 11/21/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on January 7,th, 2008. Claim 1 has been amended. Claims 1-6 and 17-26 are pending and have been considered below.

Claim Objections

2. Claim 1 is objected to because of the following informalities: claim 1 recites the limitation of "said keygen logickeygen unit". Appropriate correction is required.

Response to Arguments

3. Applicant's arguments filed January, 7th, have been fully considered but they are not persuasive. Applicant asserted that the rejection of claims 22-25 is improper under 102(e) over the Yup reference. It should be noted that the heading of the rejection contained an inadvertent typo. The rejection is an obviousness rejection under 103 over Yup et al in view of Kessler . As applicant clearly noted on page 14 of the response , the rejection was based on Yup and Kessler. Applicant assumption that the circuit of Yup could be employed to perform AES encryption and decryption is correct. The heading of the rejection has been updated, but the content of the rejection is the same. Accordingly, the rejection is maintained.

Applicant argued that "the microprocessor is not a coprocessor nor is a coprocessor a microprocessor "see response at page 16. while a microprocessor is not a co-processor. As asserted by applicant , they in the context of the claim invention , perform the same function . Te claims merely recite a microprocessor for receiving a

cryptographic instruction. The co-processor of Kessler does just that. The co-processor of Kessler includes an execution queue that fetches cryptographic instructions (Fig. 8) and therefore meets the claim limitation.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413,208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The remainder of Applicant's arguments mirror previous arguments made with respect to the independent claims and has been fully addressed above.

Ff

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-6, 8-15, 17-20 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yup et al** (2002/0191784) in view of **Kessler et al** (US 6789147).

Claim 1: **Yup et al.** discloses an apparatus for performing cryptographic operations, comprising:

i. An instruction register having a cryptographic instruction, received by microprocessor as part of an instruction flow executing on said

microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user- generated key schedule be employed for execution of said one of the cryptographic operations (page 4, paragraph [0045]);

ii. keygen unit, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to load said user-generated key schedule (page 3, paragraph [0028]).

iii. An execution unit, operatively coupled to said keygen logic, configured to employ said user-generated key schedule to execute said one of the cryptographic operations, said execution unit comprising: a cryptography unit, configured execute a plurality of cryptographic rounds on each of plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit (page 1, paragraph [0004]).

But does not explicitly disclose that the device is microprocessor. However **Kessler et al** discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in **Yup et al** to be a processor. One would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

Claim 17: **Yup et al.** discloses an apparatus for performing cryptographic operations, comprising:

i. A cryptography unit within a microprocessor, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes a key size to be employed when executing said one of the cryptographic operations *(AES block cipher can use varying key lengths)* [page 4, paragraph 0045];

ii. keygen unit, operatively coupled to said cryptography unit, configured to direct said microprocessor to perform said one of the cryptographic operations and to employ said user-generated key schedule when performing said one of the cryptographic operations (page 3, paragraph [0028].

But does not explicitly discloses that the device is microprocessor. However Kessler et al discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in **Yup et al** to be a processor. One would have been motivated to use a processor in order to maximize system flexibility and to reduce space

requirement for the design.

Claims 2 and 3: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 1 above, and **Yup et al** further discloses that said one of the cryptographic operations further comprises an encryption and decryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks *(plurality of channels with input means)* to generate a corresponding plurality of ciphertext blocks *(plurality of channels with output means)* and said decryption operation comprising decryption of a plurality of ciphertext blocks*(plurality of channels with input means)* to generate a corresponding plurality of plaintext blocks*(plurality of channels with output means)* (page 2, paragraph [0017]).

Claims 4, 18: **Yup et al** and **Kessler et al** disclose an apparatus as in claims 1, and 17 above, and **Yup et al** further discloses said user-generated key schedule is stored in memory (page 3, paragraph [0028]).

Claims 5, 19: **Yup et al** and **Kessler et al** disclose an apparatus as in claims 1, and 17 above, and **Yup et al** further discloses that said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm (page 2, paragraph [0016]).

Claims 6, 20: **Yup et al** and **Kessler et al** disclose an apparatus as in claims 1 and 17 above, and **Yup et al** further discloses that said keygen unit is configured to interpret a key generation field within a control word which is referenced by said cryptographic instruction *(the key expansion block generates a single round key by performing a single key expansion operation for each round of the AES block cipher)* (page 3, paragraph [0028]).

Claim 8: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 1 above and **Yup et al** further discloses that said cryptographic instruction implicitly references a plurality of registers within said computing device (FIG.1).

Claims 9-11: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 8 above, and **Yup et al** further discloses that said cryptographic instruction implicitly references a plurality of registers, which include a first register, wherein contents of said first register *(plaintext storage registers)* comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished (page 4, paragraph [0043]); and a second register*(cipher block output storage register)*, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of

output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks (page 4, paragraphs [0043-0044]), said third register indicate a number of text blocks within a plurality of input text blocks (page 4, paragraphs [0043-0044]).

Claim 12: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 8 above and further **Yup et al** further discloses that said plurality of registers comprises a fourth register *(cipher key storage register)*, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations (page 3, paragraph [0028]).

Claim 13: **Yup et al** and **Kessler et al** disclose an apparatus as in claims 8 above, and **Yup et al** further discloses that said user-generated cryptographic key schedule comprises said cryptographic key data *(*page 3, paragraph [0028]).

Claim 14: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 8 above and **Yup et al** further discloses that said plurality of registers comprises a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location,

contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations (page 3, paragraph [0027]). The examiner notes that **Yup et al** discloses operating the apparatus in CBC mode, which implies the use of initialization vectors. Thus, it is inherent for the initialization vectors to be stored in memory.

Claim 15: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 8 above and **Yup et al** further discloses that said plurality of registers comprises a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises: a key size field*(nk = key size)*, configured to specify said one of a plurality of cryptographic key sizes to be employed during execution of said one of the cryptographic operations*(the key expansion block generates a single round key by performing a single key expansion operation for each round of the AES block cipher)* [page 3, paragraph 0028]. The examiner notes that it is inherent for the control word to be stored in memory because the key expansion block uses it for generating a round key.

Claim 22: **Yup et al** discloses a method for performing cryptographic operations in a device, the method comprising:

i. Receiving a cryptographic instruction that prescribes employment of a user-generated key schedule during execution of one of a plurality of cryptographic operations *(*page 4, paragraph [0045]); and

ii. Employing the user-generated key schedule when executing the one of the cryptographic operations (page 3, paragraphs [0028-0035]).

But does not explicitly disclose that the device is microprocessor. However **Kessler et al** discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in **Yup et al** to be a processor. One would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

Claim 23: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 22 above, and **Yup et al** further discloses that said user-generated cryptographic key schedule comprises said cryptographic key data *(*page 3, paragraph [0028]).

Claim, 24: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 22 above, and **Yup et al** further discloses said user-generated key schedule is stored in memory (page 3, paragraph [0028]).

Claim 25: **Yup et al** and **Kessler et al** disclose an apparatus as in claim 22 above, and **Yup et al** further discloses that said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm (page 2, paragraph [0016]).

9. Claims 7, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yup et al** (2002/0191784) in view of **Kessler et al** (US 6789147) in further view of **Miller** (US 6081884).

Claims 7, 21: **Yup et al** and **Kessler et al** disclose an apparatus as in claims 1, and 17 above, while neither of them explicitly discloses that said cryptographic instruction is prescribed according to the x86 instruction format. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in the combined teaching of **Yup et al** and **Kessler et al** to implement the x86 instruction set because the x86. instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by **Miller** (Col. 2, lines 9-14).

10. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Yup et al.** (2002/0191784) in view of **Miller** (US 6081884).

Claim 26: **Yup et al** discloses an apparatus as in claim 22 above, but does not explicitly disclose that said cryptographic instruction is prescribed according to the x86 instruction format. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in **Yup et al** to implement the x86 instruction set because the x86. instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by **Miller** (Col. 2, lines 9-14).

Conclusion

2. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571)

270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Monday, Monday, March 31, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136